COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

JOHN NAIMO
AUDITOR-CONTROLLER

August 13, 2015

TO: Mitchell H. Katz, M.D., Director
Department of Health Services

FROM: John Naimo
Auditor-Controller

SUBJECT: **HIPAA AND HITECH ACT PRIVACY COMPLIANCE REVIEW – HEALTH SERVICES ADMINISTRATION HIPAA TRAINING TRACKING AND PROCESS**

We have completed a review of the Department of Health Services' (DHS) process for administering and tracking compliance with the Health Insurance Portability and Accountability Act (HIPAA) training requirements for DHS' Health Services Administration (HSA) staff.

The Auditor-Controller's (A-C) Chief HIPAA Privacy Officer (CHPO) assessed the tools and methods DHS uses to administer and track HIPAA training provided to HSA workforce members, particularly new hires and transfers from other divisions or County departments. The purpose of our review was to examine DHS' process for tracking whether HSA workforce members have complied with HIPAA training requirements pursuant to the regulations and DHS' policies and procedures. Because the County is currently developing a new HIPAA training curriculum, we did not review the content or adequacy of DHS' training materials. We interviewed DHS' Privacy Officer, and various staff from the DHS Audit and Compliance Division, Human Resources Division (DHS HR), and Application Development Department. We also reviewed pertinent DHS policies and training records.

On June 24, 2015, we provided your Department with our final draft report. DHS Audit and Compliance staff declined to participate in an exit conference, as they generally agreed with our findings and recommendations.

Background

HSA is responsible for performing the centralized administrative functions of DHS, which includes Human Resources, Finance, Information Technology, Audit and Compliance, and Executive Management and staff. As of February 2, 2015, HSA had 1,348 staff, all of whom are required to complete DHS' HIPAA Privacy and Security training.

Each HIPAA covered department designates its own privacy officer to implement and fulfill the obligations of the County's HIPAA privacy program within the department. Among other duties, DHS' Privacy Officer is responsible for ensuring that DHS' workforce, including staff housed at HSA and the hospitals and clinics, successfully completes HIPAA training. DHS' training addresses HIPAA and State privacy and security requirements, as well as DHS' related policies and procedures.

HIPAA Training Requirements

The HIPAA regulations[1] require that covered entities provide HIPAA training to all members of its workforce, including employees, volunteers, and executive management as necessary and appropriate to perform their functions. Documentation that the training was provided must be maintained in written or electronic form for six years.

DHS' Privacy Officer told us that the Joint Commission, an independent organization that accredits and certifies health care organizations such as DHS, requires that health care personnel complete all training within 30 days of beginning employment. DHS requires that employees receive HIPAA training within 30 days, in order to meet the Joint Commission standard. Because the employee onboarding process, which includes HIPAA training, can be delayed due to technical issues and employees may need access to protected health information (PHI) before completing it, DHS provides all new employees with a privacy packet and training handbook during orientation, as per DHS Policy 361.24 – Privacy and Security Awareness and Training Policy. The training handbook is considered a short-term solution to meet the minimum training requirements. However, the policy does not explicitly state that new employees must receive the privacy packet and training handbook as required by the Joint Commission. In addition, DHS' Privacy Officer monitors employees to ensure they complete the Department's web-based HIPAA Privacy and Security training within 60 days of employment. However, this requirement is also not specifically stated in DHS Policy 361.24.

Employees must also complete a refresher course when there are significant changes to the HIPAA regulations or County or DHS policies. HIPAA covered entities and their respective training programs are subject to audit by various agencies, including the A-C,

[1] 45 CFR §164.308

the California Department of Public Health, and the U.S. Department of Health and Human Services' Office for Civil Rights.

Recommendations

Department of Health Services Management:

1. **Update Department of Health Services Policy 361.24 to ensure that managers/supervisors are aware of the requirement for new and transferred staff to acknowledge receipt of the privacy packet and training handbook within 30 days to satisfy the Joint Commission standards.**

2. **Ensure that managers receive timely notice of staff who require Health Insurance Portability and Accountability Act Privacy and Security web-based training, so that they can follow-up to ensure that employees have completed it within 60 days of hire or transfer.**

Results of Review

Onboarding

According to DHS HR staff, during the onboarding process at HSA new hires and transfers are provided with a brief orientation, including a HIPAA privacy packet and training handbook. DHS' Privacy Officer stated that the HIPAA privacy packet contains County and Departmental policies on safeguarding PHI, acceptable use of County information technology resources, breach reporting, and disciplinary actions. Employees must attest that they have read and understand the information in the packet. We reviewed personnel files for 28 HSA employees and noted that each contained the attestation, signed either during onboarding or, for those staff who joined DHS prior to HIPAA, at a later date.

We also reviewed a sample onboarding packet, and noted that it included applicable DHS policies related to HIPAA and appears to meet the requirements of the standards.

Training

Currently, DHS' Privacy Officer is responsible for creating and updating the Department's HIPAA Privacy and Security training, which is accessed through DHS' Intranet site. Because the County's Chief Information Office is currently negotiating with a contractor to develop a new HIPAA training curriculum, with the goal of creating a single training curriculum applicable to all County employees, we did not evaluate the content or adequacy of DHS' training materials. Our purpose was to evaluate the process by which DHS delivers its HIPAA training to HSA employees, and tracks that training, to ensure employees complete it pursuant to DHS Policy 361.24.

DHS' Privacy Officer stated that all HSA workforce members must complete the Department's web-based HIPAA Privacy and Security training within 60 days of beginning employment or transferring-in, including an examination on which employees must answer all (100%) questions correctly to pass. DHS management indicated that third-party training or HIPAA training provided by other agencies may not be substituted for the DHS training because the Department is required to train its workforce on its own policies and procedures, in addition to the HIPAA regulations. The County's current HIPAA training, which is accessed via the Learning Management System, only addresses federal requirements, and not State requirements or DHS policies and procedures.

In addition to the initial HIPAA training and periodic refresher courses, HSA and DHS HR staff told us that during the annual performance evaluation process, workforce members are required to review several policies: DHS' Safeguards for Protected Health Information (Policy No. 361.23); Acceptable Use of County Information Technology Resources (Policy No. 935.20); Disciplinary Actions for Failure to Comply with Privacy Policies and Procedures (Policy No. 361.10); and, Reporting Privacy and Security-Related Breaches (Policy No. 361.11). We reviewed the policies and noted that they appear to address the requirements of the HIPAA training standards within their respective topics.

Tracking

DHS' Privacy Officer told us that she is responsible for tracking whether HSA employees have completed the required HIPAA Privacy and Security training. The DHS Application Development Department provides the Privacy Officer a monthly report detailing the training status of every DHS employee, including new hires and transfers. The report identifies employees by department code (i.e., 110 for HSA, 130 for High Desert Hospital, etc.) and pay location, allowing the DHS Privacy Officer to identify employees who have not yet completed the training. The report also assists in identifying compliance trends.

DHS' Privacy Officer stated that she contacts the supervisors of non-compliant employees to determine whether the employees have a legitimate reason (e.g., approved leave) that prevented them from completing the training. Also, DHS' Privacy Officer confirms with DHS' HR whether certain non-compliant employees are new hires or transfers, or are absent for reasons such as military deployment, long-term leave, etc. DHS' Privacy Officer told us that she sorts the data by training date of completion and determines whether any employee on the list has not taken the HIPAA training.

DHS' Privacy Officer provided us with the HIPAA Privacy and Security training report for HSA staff as of February 2, 2015. The report indicated that 1,315 (98%) of 1,348 HSA staff had completed the HIPAA Privacy and Security training. The 33 remaining staff

were either new employees who were within 60 days of their hire/transfer date, or on long-term leave.

We reviewed a sample of prior period training reports from 2014 and 2015, and randomly selected 57 HSA employees from those reports for additional review. Specifically, we used the County's electronic Human Resources System (eHR) to determine when the employees entered DHS service, either as new hires or as transfers, and compared that start date with their training completion date to determine whether they completed HIPAA training within the required timeframe. We noted that 16 (28%) of 57 employees reviewed did not complete the training within 60 days.

We inquired with DHS' Privacy Officer about why those 16 employees did not complete HIPAA training within the required timeframe. She stated that managers are responsible for ensuring that their subordinates complete mandatory trainings, including the HIPAA Privacy and Security training. DHS' Privacy Officer stated that she will work with DHS Audit and Compliance Division and DHS HR to ensure that employees complete HIPAA training within 60 days of being hired or transferring to HSA.

Conclusion

Overall, it appears that HSA is complying with the HIPAA training requirements and related County policies. Specifically, HSA appears to have controls and business processes in place to determine whether workforce members requiring HIPAA training are identified, and that documentation is maintained for all completed training. However, our review noted that some employees had not completed the training within 60 days of joining HSA. Thus, we have made recommendations to ensure that HSA continues to maintain a high standard for its HIPAA Privacy and Security training program.

We shared our findings with DHS management on June 24, 2015. DHS' Audit and Compliance Division reviewed our findings and indicated general agreement with our findings and recommendations.

We wish to thank DHS' Privacy Officer, managers, and staff for their cooperation and assistance during this review. Please call me if you have any questions, or your staff may contact Linda McBride, Chief HIPAA Privacy Officer, at (213) 974-2166.

JN:RGC:GZ:LTM:TW

c: County Counsel
Chief Information Office
Audit Committee
Health Deputies